CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being submitted *via* the USPTO EFS Filing System on the date shown below to **Mail Stop Appeal Brief - Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: May 7, 2007 /Jessica Sexton/
Jessica Sexton

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:			
Applicant(s):	Matthew Charles Priestley *et al.*	Examiner:	Shanto Abedin
Serial No:	10/083,010	Art Unit:	2136
Filing Date:	February 26, 2002		

Title: SYSTEM AND METHOD TO PACKAGE SECURITY CREDENTIALS FOR LATER USE

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Applicant submits this brief in connection with an appeal of the above-identified patent application. Payment is being submitted via credit card in connection with all fees due regarding this appeal brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP319US].

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Microsoft Corporation, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellants, appellants' legal representative, and/or the assignee of the present application are not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1, 3-18, 20-29 and 31-33 stand rejected by the Examiner. The rejection of claims 1, 3-18, 20-29 and 31-33 is being appealed.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

No claim amendments have been entered subsequent the Final Office Action dated December 7, 2006.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))

A. Independent claim 1

Independent claim 1 recites a computer implemented system for processing credentials, comprising the following computer executable components: a wrapper that packages credentials associated with resources of a service and a pass-phrase employed in connection with generation of the wrapper *via* a cryptographic wrapping key, the pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service, and the pass-phrase distributed separately from the credentials. (*See e.g.* Figure 1, and corresponding text at pg. 6 ll. 19-27)

B. Independent claim 18

Independent claim 18 provides for a method to facilitate a security connection between entities. A strong set of security credentials are wrapped to house them in order to mitigate

exposure of the credentials to a party non-related to the transaction *via* a method of generating a strong password; generating a pass-phrase; wrapping the password cryptographically *via* the pass-phrase; storing the wrapped password in an executable; and transmitting the executable and the pass-phrase to a system *via* different communications mediums. (*See e.g.,* Pg. 12 l.21 – pg. 13 l. 12)

C. Independent claim 27

Independent claim 27 recites a computer executable system to facilitate a security relationship between parties, comprising: computer implemented means for generating a password, computer implemented means for generating a pass-phrase, computer implemented means for generating a package of credentials, computer implemented means for storing the password separate from the package, computer implemented means for locking the package with the pass-phrase, and computer implemented means for transmitting the package and the pass-phrase to a system *via* different communications mediums. (*See e.g.*, Pg. 6 l.19 – pg. 8 l. 20)

D. Independent claim 28

Independent claim 18 provides for a computer-readable medium having stored thereon a signal to communicate security data between at least two nodes, comprising: a first data packet comprising: a password component employed to establish a trust relationship between at least two nodes; and a wrapper field employed to encapsulate the password, the wrapper field mediating access to the password; and a second data packet comprising: a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field. (*See e.g.*, Pg. 11, l.16 – pg.12. l.10)

E. Independent claim 31

Independent claim 31 recites a computer implemented system to establish a trust relationship, comprising the following computer executable components, a service that controls one or more resources, the service issues credentials to facilitate access to the resources; a wrapper generated by the service to package the credentials; and a pass-phrase employed to generate the wrapper and mediate access to the service, the pass-phrase distributed separately from the credentials. (*See e.g.*, Pg. 11, l.16 – pg.12. l.10)

F. Independent claim 33

Independent claim 33 recites: A computer-readable medium having stored thereon a data structure, comprising: a first data field containing cryptographic data associated with a password; a second data field containing cryptographic data associated with a pass-phrase, the pass-phrase employed to mitigate exposure of the password to non-trusted entities; and a third data field containing a wrapper employed to encapsulate the password, the wrapper generated by the pass-phrase and distributed separately from the pass-phrase to facilitate a security connection between entities. (*See e.g.*, Pg. 6 l.19 – pg. 8 l. 20)

The aforementioned means for limitations are identified as claim elements subject to the provisions of 35 U.S.C. §112 ¶6. The corresponding structures are identified with reference to the specification and drawings in the parentheticals above corresponding to those claim limitations.

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1, 3-9, 17, 18, 20, 23 and 29 are unpatentable under 35 U.S.C. §103(a) over Lee *et al.* ("A secure electronic software distribution (ESD) protocol based on PKC" by Lee *et al.*, EC-Web 2000, LNCS 1875, pp. 63-71, 2000), in view of Hypponen (U.S. 6,986,050 B2), and further in view of Bathrick *et al.* (U.S. 5,825,300).

B. Whether claims 10-12 are unpatentable under 35 U.S.C. §103(a) over Lee *et al.*, in view of Hypponen, in view of Bathrick *et al.*, and further in view of Brainard (SecurSight: An architecture for secure information access, RSA Lab).

C. Whether claims 27, 28, 31 and 33 are unpatentable under 35 U.S.C. §103(a) over Lee *et al.*, in view of Bathrick *et al.*

D. Whether claims 13-16, 21, 22, 24, 25 and 32 are unpatentable under 35 U.S.C. §103(a) over Lee *et al.*, in view of Hypponen, and further in view of Bathrick *et al.* and Brainard.

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1, 3-9, 17, 18, 20, 23 and 29 Under 35 U.S.C. §103(a)

Claims 1, 3-9, 17, 18, 20, 23 and 29 stand rejected as obvious under 35 U.S.C. §103(a) over Lee *et al.* ("A secure electronic software distribution (ESD) protocol based on PKC" by Lee *et al.*, EC-Web 2000, LNCS 1875, pp. 63-71, 2000), in view of Hypponen (U.S. 6,986,050 B2), and further in view of Bathrick *et al.* (U.S. 5,825,300). Reversal of this rejection is respectfully requested for at least the following reasons. Lee *et al,* Hyppopen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

> To reject claims in an application under §103, an examiner must show an unrebutted *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicants' disclosure. *See In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. This is achieved by providing a strong set of security credentials between a master entity such as a service and a remote entity such as a partner. In conjunction with the strong set of security credentials, a protocol is provided that acts as a package, wrapper or container to house the security credentials before delivery from the service to the partner to facilitate secure communications between the parties. To this end, independent claims 1, 18 and 28 recite similar features. In particular, independent claim 1 recites *a system and method for facilitating a computer a security connection between entities, comprising a wrapper that packages credentials associated with resources of a service; and a pass-phrase employed in connection with generation of the*

wrapper via a cryptographic wrapping key, ***the pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service, and the pass-phrase distributed separately from the credentials.*** Lee *et al.,* Hypponen and Bathrick, individually or in combination, fail to teach or suggest such aspects of the claimed invention.

Lee *et al.* discloses a secure electronic software distribution protocol based on public key cryptography (PKC). At page 5 of the Final Office Action, the Examiner contends that Lee *et al.* discloses a wrapper that packages credentials associated with resources of a service. Appellants' representative disagrees. In accordance with the claimed invention, the credentials packaged in the wrapper are those credentials employed by the service as proof that the holder should be granted access to the resources. On the contrary, Lee *et al.* packages a software in the wrapper, the software being the resource offered to the customer. For example, Lee *et al.* teaches generation of the hash function at the AA (authentication agent) after receiving the customer ID and password from a user (*See* Lee *et al.* page 6 lns .12-14). Hence, the 'secret' used in the hash function as taught by Lee *et al.* is used to verify the customer ID and password rather than provide access to the customer ID and password. Thus, Lee *et al.* is silent regarding ***the pass-phrase employed to facilitate access to the credentials*** as recited by the subject claims.

At page 5 of the Final Office Action, the Examiner concedes that Lee *et al.* does not teach a pass phrase employed in connection with generation of cryptographic wrapping key, the pass phrase distributed separately from the credentials. The Examiner attempts to compensate for the aforementioned deficiencies of Lee *et al.* with Hypponen and Bathrick *et al.* Hypponen discloses a two-level mechanism of securing data stored in an electronic device comprising encrypting the data using a cryptographic key generated from a passphrase as well as a password to provide access to data. A user is asked to enter a password and a passphrase, the system uses the pass-phrase to generate a cryptographic key, stores it in the system and uses it to encrypt and decrypt the data (*See* Hypponen col.2 lns. 45-60). In contrast, the cryptographic wrapping key generated from the pass-phase of applicant's claimed invention is employed in generating the wrapper that actually wraps credentials that provide access to resources rather than resources themselves. Nowhere does Hypponen teach or suggest wrapping the password using the cryptographic key generated by the pass-phrase. Thus, Hypponen is silent regarding ***the pass-phrase employed to facilitate access to the credentials*** as recited by the subject claims.

Bathrick *et al.* teaches computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain. The certifying authority generates keying material, which includes a password and sends it to the subject entity via manual courier or other means that is different from the communication system operating through a network (*See* Bathrick *et al.* col.2 lns. 34-40). Hence, Bathrick *et al.* teaches securing a password by communicating it through non-electronic media rather than a ***pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service, and the pass-phrase distributed separately from the credentials*** as recited in applicants' subject claims. Therefore, it can be concluded that Bathrick *et al.* does not teach or suggest that the pass phrase is distributed separately from the credentials. Generating a pass-phrase for wrapping the credentials as taught in the subject claims provides additional security to the credentials hence mitigating the need to protect the credentials by communicating them through non-electronic means as taught by Bathrick *et al.*

In view of at least the foregoing, it is apparent that Lee *et al,* Hyppopen and Bathrick *et al.*, do not teach or suggest every aspect of appellants' claimed subject matter as taught by independent claims 1, 18 and 28 (and claims which depend there from). Accordingly, it is requested that this rejection should be reversed.

B. Rejection of Claims 10-12 Under 35 U.S.C. §103(a)

Claims 10-12 stand rejected as obvious under 35 U.S.C. §103(a) over Lee *et al.*, in view of Hypponen, in view of Bathrick *et al.*, and further in view of Brainard (SecurSight: An architecture for secure information access, RSA Lab). It is respectfully submitted that this rejection should be reversed for the following reasons. Claims 10-12 depend from independent claim 1. As discussed *supra*, Lee *et al.,* Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in claim 1. In particular, Brainard does not make up for the deficiencies of Lee *et al,* Hypponen and Bathrick *et al.* with respect to independent claim 1 (from which claims 10-12 depend). Thus, it is respectfully submitted that this rejection be reversed.

C. Rejection of Claims 27, 28, 31 and 33 Under 35 U.S.C. §103(a)

Claims 27, 28, 31 and 33 stand rejected as obvious under 35 U.S.C. §103(a) over Lee *et al.*, in view of Bathrick *et al.* It is respectfully submitted that this rejection should be reversed for the following reasons. Lee *et al.*, and Bathrick, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

Independent claims 27, 28, 31and 33 recite similar limitations namely, *a computer-readable medium having stored thereon a signal to communicate security data between at least two nodes, comprising a first data packet comprising a password component employed to establish a trust relationship between at least two nodes* ***and a wrapper field employed to encapsulate the password****, the wrapper field mediating access to the password and a second data packet containing* ***a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field.*** Lee *et al.* and Bathrick *et al.* are silent about such novel aspects of the applicants' subject claims.

As discussed *supra*, Lee *et al.* does not disclose or suggest transmitting the wrapper field for the credentials separately from the pass-phrase. Bathrick *et al.* does not make up for the aforementioned deficiencies of Lee *et al.* At various sections of the Final Office Action dated December 7, 2006, it is contended that Bathrick *et al.* teaches the distributing the pass-phrase separately from the wrapper field as it teaches communicating key and certificate material separately (*See* Final Office Action dated December 7, 2006 page 6 lines 7-8, page 12 lns. 12-13). However, it is submitted that the claimed pass-phrase which is used to generate a wrapper for the credentials as recited in the claims is not the same as the password disclosed by Bathrick *et al.* This is because, the password of Bathrick *et al.* is only used to protect data transferred between and an entity and a certifying authority rather than generate a wrapper for such credentials (*See* Bathrick *et al.* col.2 lns. 23-25). Therefore, Lee *et al.* and Bathrick *et al.* individually or in combination do not teach ***a wrapper field employed to encapsulate the password, a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field*** as recited by applicants' subject claims. Accordingly, reversal of this rejection is requested.

D. Rejection of Claims 13-16, 21, 22, 24, 25 and 32 Under 35 U.S.C. §103(a)

Claims 13-16, 21, 22, 24, 25 and 32 stand rejected as obvious under 35 U.S.C. §103(a) over Lee *et al.*, in view of Hypponen, and further in view of Bathrick *et al.* and Brainard. It is respectfully submitted that this rejection should be reversed for the following reasons. Claims 13-16 depend on independent claim 1, claims 21, 22, 24, 25 depend on independent claim 18 and claim 32 depends on independent claim 31. As stated *supra*, Lee *et al.*, Hypponen, Bathrick *et al.* and Brainard, individually or in combination, do not teach or suggest each and every element set forth in the subject independent claims. In particular, Brainard relates to an architecture that combines authentication, authorization and secure communication but does not make up for the aforementioned deficiencies of Lee *et al.* and Bathrick *et al.* with respect to independent claims 1, 18 and 31 (which claims 13-16, 21-22, 24-25 and 32 depend from). Accordingly, reversal of this rejection is requested.

E. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of claims 1, 3-18, 20-29 and 31-33 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP319US].

Respectfully submitted,
AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24th Floor, National City Center
1900 East 9th Street
Telephone: (216) 696-8730
Facsimile: (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A computer implemented system for processing credentials, comprising the following computer executable components:

a wrapper that packages credentials associated with resources of a service; and

a pass-phrase employed in connection with generation of the wrapper *via* a cryptographic wrapping key, the pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service, and the pass-phrase distributed separately from the credentials.

2. (Canceled)

3. The system of claim 1, the credentials providing stronger encryption than the pass-phrase.

4. The system of claim 3, the credentials providing greater than 100 bits of encryption.

5. The system of claim 3, the pass-phase having human-readable alpha-numeric characteristics.

6. The system of claim 1, further comprising one or more partners to request access to the resources.

7. The system of claim 6, at least one of the partners includes a credential store to manage the credentials.

8. The system of claim 7, the at least one partner distributes the credentials to at least one other partner in order to facilitate access to the resources of the service.

9. The system of claim 1, the pass-phase is at least one of spoken, displayed on a screen and typed.

10. The system of claim 1, further comprising at least one of a Secure Socket Layer (SSL), a Virtual Private Network (VPN), and a dedicated line to establish connections to the service.

11. The system of claim 10, further comprising a remote login utilizing a basic authentication over the SSL.

12. The system of claim 10, further comprising at least one SSL certificate to establish connections to the service.

13. The system of claim 1, the services are associated with a platform provisioning service.

14. The system of claim 13, the platform provisioning service associated with at least one partner, the partner including at least one of a tenant and a service provider to form at least one of a billing, a financial, and an accounting service.

15. The system of claim 14, the partner employs the pass-phrase to unlock the credentials and achieve access to the platform provisioning services.

16. The system of claim 14, at least one of the platform provisioning service and the partner maintain an account to process the credentials, the at least one of the platform provisioning service and the partner employ a Universal Resource Locator (URL) to present the credentials to the account.

17. A computer-readable medium having computer-executable instructions stored thereon to perform at least one of processing and the generation of the wrapper and the pass-phrase of claim 1.

18. A method to facilitate a security connection between entities, comprising:
generating a strong password;
generating a pass-phrase;
wrapping the password cryptographically *via* the pass-phrase;
storing the wrapped password in an executable; and
transmitting the executable and the pass-phrase to a system *via* different communications mediums.

19. (Canceled)

20. The method of claim 18, further comprising employing the pass-phrase to unlock the strong password stored in the executable, the strong password employed to establish a trust relationship with an entity.

21. The method of claim 18, further comprising at least one of:
requesting a Secure Sockets Layer (SSL) connection; and
presenting an SSL certificate in response to the request.

22. The method of claim 21, further comprising at least one of:
verifying an SSL certificate;
requesting a Universal Resource Locator (URL) from a listener;
presenting authentication credentials to a receiver; and
logging in a caller to an account.

23. The method of claim 18, further comprising limiting access to the executable.

24. The method of claim 18, further comprising at least one of:
setting up account privileges;
designating account contacts; and
verifying the contacts.

25. The method of claim 24, further comprising verbally communicating the pass-phrase.

26. The method of claim 25, further comprising transmitting and storing the password and the pass-phrase separately.

27. A computer executable system to facilitate a security relationship between parties, comprising:

computer implemented means for generating a password;

computer implemented means for generating a pass-phrase;

computer implemented means for generating a package of credentials;

computer implemented means for storing the password separate from the package;

computer implemented means for locking the package with the pass-phrase; and

computer implemented means for transmitting the package and the pass-phrase to a system *via* different communications mediums.

28. A computer-readable medium having stored thereon a signal to communicate security data between at least two nodes, comprising:

a first data packet comprising:

a password component employed to establish a trust relationship between at least two nodes; and

a wrapper field employed to encapsulate the password, the wrapper field mediating access to the password; and

a second data packet comprising:

a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field.

29. The signal of claim 28, wrapper field being cryptographically weaker than the password.

30. (Canceled)

31. A computer implemented system to establish a trust relationship, comprising the following computer executable components:

a service that controls one or more resources, the service issues credentials to facilitate access to the resources;

a wrapper generated by the service to package the credentials; and

a pass-phrase employed to generate the wrapper and mediate access to the service, the pass-phrase distributed separately from the credentials.

32. The system of claim 31, the service is a provisioning service that establishes a trust relationship between one or more partners *via* the credentials.

33. A computer-readable medium having stored thereon a data structure, comprising:

a first data field containing cryptographic data associated with a password;

a second data field containing cryptographic data associated with a pass-phrase, the pass-phrase employed to mitigate exposure of the password to non-trusted entities; and

a third data field containing a wrapper employed to encapsulate the password, the wrapper generated by the pass-phrase and distributed separately from the pass-phrase to facilitate a security connection between entities.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.